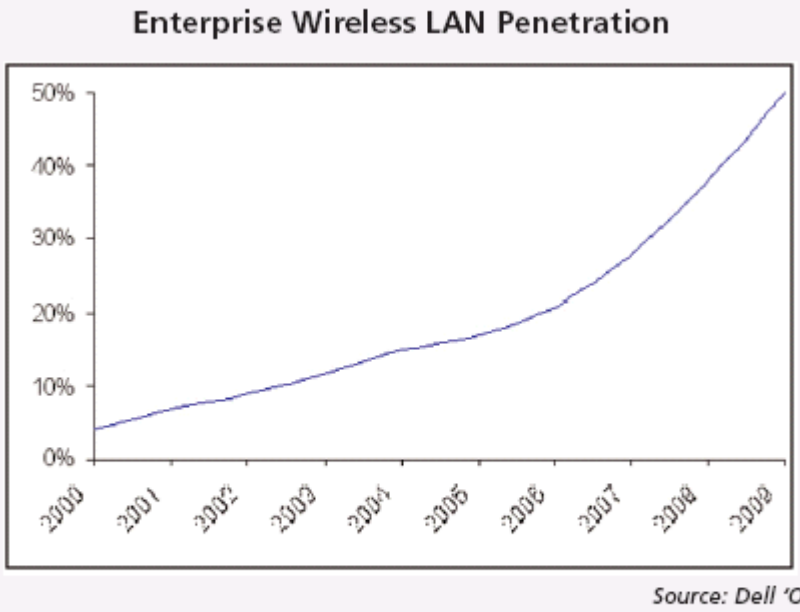
The Business Justification for Wireless Intrusion Prevention

More and more companies are realizing that their corporate air waves are an asset that requires protection. Strong security policies have been created for wired networks – protection systems such as firewalls, IDS, anti-virus and anti-spam systems are put in place and policies are monitored for compliance. The same is now needed for the corporate air waves. The proliferation of Wi-Fi makes it nearly impossible for today's enterprise to remain unaffected by this technology. Wireless LAN capability shipped in over 90% of laptops*1* in 2005. Due to the prevalence of wireless LAN infrastructure in neighboring buildings, cafes and retail stores, it is now common to be within range of half a dozen or more Wi-Fi networks at the same time. Even if corporate policy dictates 'no Wi-Fi', networks and users both need to be protected from a wide variety of wireless threats (rogue Access Points, unintentional client associations, ad-hoc networks, etc.).

A strong security policy was created to protect the corporation's assets from abuse over the wireline network. The new reality of wireless technology means that maintaining that same level of protection now requires considering threats via the corporate airwaves. To protect your corporate air waves, you need to:

- define a wireless policy
- enforce that policy, and
- audit and demonstrate compliance to the policy



The exponential growth of wireless LAN technology means every corporation will be exposed to wireless threats, whether they have a 'no Wi-Fi' policy or not.

The Financial and Legal Consequences of a Weak Wireless Security Policy
The penalties for a lax wireless security policy, compliance and monitoring program can be much greater than embarrassment. As was recently ruled on by the Federal Trade Commission2, Discount Shoe Warehouse (DSW), a major retailer of men's and women's shoes, now faces significant financial penalties and the imposition of a twenty (20) year monitoring plan of their security policy and compliance procedures. A key problem in their security processes was "failing to use readily available security measures to limit access to its computer networks through wireless access points on the networks...and failing to employ sufficient measures to detect unauthorized access." In addition to imposition of a of $6.5 to $9.5 million fine, the company has spent considerable IT, PR and legal resources on this issue. Deployment of a wireless intrusion prevention system could have providing warning, as well as prevented, the security lapse through wireless access points.

Corporations have good business and legal reasons for setting up security policies and stringent compliance plans. Strong security policies need to be developed, implemented and monitored for abuse. A corporation that fails to monitor for policy abuse is missing an important component of security. Thus, wireless perimeter intrusion detection software must be installed on a network, because it monitors for abuse of policy. Delaying an investment in wireless perimeter intrusion detection software leaves a company open to litigation, fines, prolonged audit requirements as well as loss of business, good will and corporate image. The risks to the corporation for not enforcing a wireless perimeter security policy include:

• loss of trade secrets and company confidential material
• unauthorized Internet access to pornography and gambling sites
• network outages due to Denial of Service attacks
• loss of customer or employee data leading to…
- legal and financial penalties
- damage to brand and PR issues
• connection hijacking and introduction of viruses or other malicious traffic

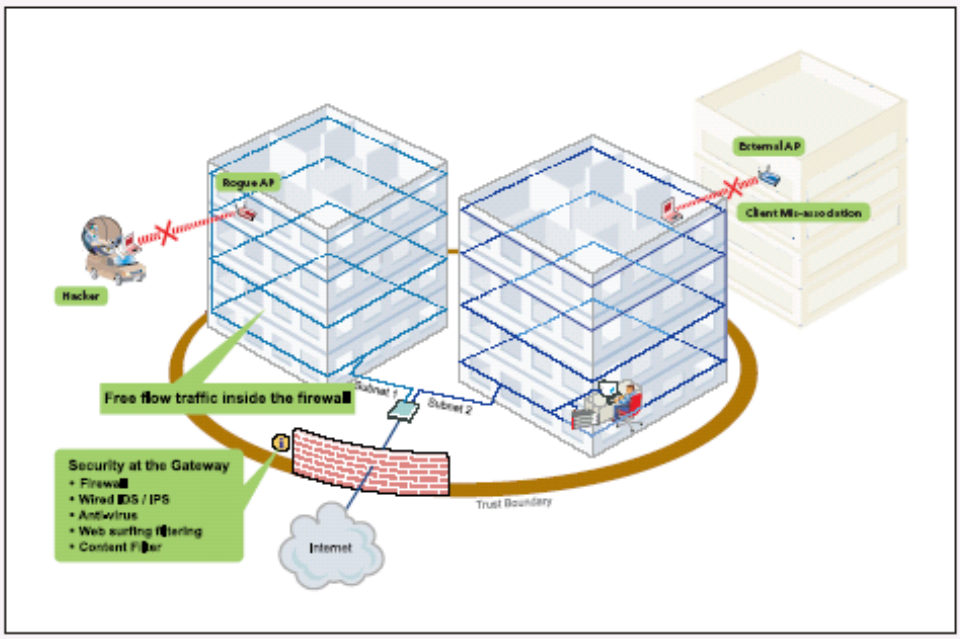
Corporations spend a significant portion of each year's budget to protect their wired networks. The same threats can be launched via the wireless medium. Best practices dictate a multi-layered approach, using best-of-breed technology to protect against threats launched from within as well as outside the physical perimeter.

Identify Theft Over the Wireless LAN
Because wireless signals extend beyond the physical perimeter of the building, wireless security becomes even more important. Case in point is Lowe's Home Improvement which found its network hacked by two men sitting in their parking lot using offthe- shelf wireless hardware3. While ultimately arrested and successfully prosecuted, the men were able to break into the national computer system, obtain customer credit card information and install a program that altered the way credit card information was processed. A wireless perimeter security system would have blocked any unauthorized client connections to authorized access points. Furthermore, accurate location tracking would reveal the hackers' location outside the building.

A 'No Wi-Fi' Policy without Compliance Monitoring Poses A Security Risk

Just as with wireline security threats, internal users pose an equivalent if not greater risk to the enterprise than external hackers. C.E. Unterberg Towbin, a major investment bank in New York, implemented a strict 'no Wi-Fi' policy. A newly-deployed wireless perimeter security system discovered that employees with laptops were connecting to a neighboring hot spot. This allowed employees to engage in unmonitored email transactions, potentially exposing the bank to financial and legal penalties for improper disclosure of confidential customer or financial information. The wireless perimeter security system was able to enforce and monitor the 'no Wi-Fi' policy. When in the future the bank implements a wireless LAN, the wireless security system will grow with them, enforcing new wireless LAN security policies and defending against wireless threats.

Similar to wireline protection, a layered approach using wireless perimeter intrusion detection is required to monitor, detect, prevent, and report wireless vulnerabilities. Protection and auditing of the corporate air waves is then a simple matter of extending the risk management already in place for the wireline network and ensuring that investment is not diluted by low-cost and unauthorized Wi-Fi devices. Lacking such protection, organizations risk poor public relations, negative customer perception and lower stock valuation.



A rogue access point or client mis-association can bypass all wireline security methods – firewalls, VPNs, IDS/IPS, content management - leaving the enterprise open to unauthorized use, or worse, malicious attack.